UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/056,905	11/13/2001	Jurgen Bussert	A34729 (071308.0250)	2357

31625 7590 08/28/2007

BAKER BOTTS L.L.P.
PATENT DEPARTMENT
98 SAN JACINTO BLVD., SUITE 1500
AUSTIN, TX 78701-4039

EXAMINER	
PATEL, NIRAV B	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
08/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/056,905
Filing Date: November 13, 2001
Appellant(s): BUSSERT, JURGEN

Andreas Grubert
Reg. No. 59,143
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed May 16, 2007 appealing from the Office action mailed Oct 18, 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Redman et al. (U.S. Pat. No. 5,978,476 – Nov. 2, 1999)

Parlour et al. (US Patent 6,904, 527 – Jun 7, 2005)

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

Claims 1-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pat. No. 5,978,476 to Redman et al. (hereinafter "Redman") and further in view of US Patent 6,904, 527 to Parlour et al. (hereinafter "Parlour").

As per claims 1 and 8, Redman teaches a method and a system for transferring control programs comprising:

encrypting a control program code in a first development system (Figure 2 and associated text, col. 5, lines 10-19, i.e. generation of encrypted design file, see also col. 10, lines 54-59, the vendor encrypts his design file (control program) using a design file encryption system), transferring the encrypted control program code from the first development system to a second development system (col. 4, lines 41-45, the vendor creates the encrypted design file 103 makes it freely available via download on the World Wide Web), and decrypting the encrypted control program code in the second development system (Figure 4 and associated text, col. 6, line 65 67, col. 7, lines 27-29, decryptor 403 within the permission verification system 109 decrypts the authorization code 115 and decodes the encrypted design file using the design decryption key), wherein the decryption of the encrypted control program code is carried out following editing of the encrypted control program code in the second development system (col.

7, line 55 through col. 8, line 17, design processor 413 performs steps P, Q, R, S, T and U (i.e. editing of the encrypted design file) prior to decrypting the encrypted design file).

Redman does not teach (as argued by the Applicant, page 7 of the REMARK) " encrypting a part of the control program code" and decrypting the partially encrypted control program.

However, in an analogous art, Parlour teaches encrypting a part of the control program (col. 4, lines 34-44, i.e. encrypting the IP module portion of the bitstream) and decrypting the partially encrypted control program code (col. 4, lines 45-52, i.e. "the target PLD uses the key number to retrieve the proper IP module key from the non-volatile memory, and then uses the retrieved IP module key to decrypt the IP module portion. When the IP module portion has been decrypted, the resulting configuration data bitstream is used to configure the target PLD so as to realize the user-specific circuit.").

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method and system of Redman to that of Parlour for encryption a part of a control program code and decrypting the partially encrypted control program to prevent replicating the user's specific design by unscrupulous second user 's copied bitstream to configure another product (see Parlour, col. 2, lines 17-26).

As per claims 2 and 9, Redman as modified teaches the method and the system according to claims 1 and 8 respectively, further comprising exporting the encrypted control program code in a format that can be read by standard Internet clients

via the first development system, and importing a data in the format that can be read by standard Internet clients via the second development system (Redman, col. 4, lines 41-45, the encrypted design file can be freely available via download on the World Wide Web (i.e. Standard Internet clients), Kolouch, col. 5, lines 13-60).

As per claims 3 and 10, Redman teaches the method and the system according to claims 1 and 8 respectively, wherein the encryption and decryption of the data is carried out by means of asymmetrical keys (col. 5, lines 32-33).

As per claim 4, Redman teaches the method according to claim 1, wherein the encryption of the control program code is carried out following editing of the control program code in the first development system (Figure 2, file header assembler 209 (editor), col. 5, line 63 through col. 6, line 23, accepts information and generate tags A and B to be placed in a file header into the encrypted design file, prior to encrypting the design file (control program)).

As per claim 5, Redman teaches the method according to claim 1, wherein a head part of the control program remains unencrypted (col. 5, line 63-66, i.e. the file header (unencrypted) is appended to encrypted design file (col. 6, lines 27-28)).

As per claims 6, 12, 13 and 16, Redman does not teach but Parlour teaches wherein the control program comprises a plurality of program modules and wherein different modules are encrypted differently (or with different encryption level) (Parlour col. 3, lines 40-63, where public/private keys are specific to unique device identifier (UDI).

The Examiner provides the same rationale as provided in claims 1 and 8 above for combination of Redman -Parlour.

As per claims 7, Redman teaches a method and for the configuration, project engineering and commissioning of a control system and a drive comprising transferring a control program according to claim1, comprising compiling the decrypted control program, and processing the compiled control program by means of a microprocessor (Figure 5 and associated text, compiler 503, col. 8, line 64 through col. 9, line 3. performs requested actions for which the user has permission.).

As per claim 11, once modified, Redman teaches the system according to claim 8, wherein the first development device further comprises a second editor for editing the control program code (col. 5, line 63 through col. 6, line 23, i.e. a file header assembler (editor)) and a communication device (col. 4, lines 44-46, Redman discloses that encrypted design file 103 is freely available to the pubic via download on the World Wide Web (i.e. a communication device)) and a postprocessor (Figure 2 and associated text, i.e. ENCRYPTOR 203 encrypts design files after assembler (editor) accepts information and generate tags A and B to be placed in a file header into the encrypted design file) for partially encrypting the control program code connected between said second editor and communication device.

As per claim 14, Redman teaches the system according to claim 8 utilized in an arrangement for the configuration, project engineering and commissioning of a control system and/or a drive (col. 1, lines 18-32, Redman discloses the implementation of his

invention in the area of Electronic Logic Design where the designers of logic devices program programmable logical devices).

As per claim 15, Redman teaches a method and a system according to claims 6 and 13 respectively, wherein a head part of the control program remains unencrypted (col. 5, line 63-66, i.e. the file header (unencrypted) is appended to encrypted design file (col. 6, lines 27-28)).

(10) Response to Argument

Appellant's arguments filed May 16, 2007 have been fully considered but they are not persuasive.

Regarding to the Appellant's argument to claims 1 and 8 that neither Redman nor Parlour teach or suggest the claim limitation "*editing of the partially encrypted control program code...*" . Examiner disagrees with the Appellant for the above argument since Redman's invention provides the protection of intellectual property by creating the encrypted design file (control program code) and providing authorization code. As shown in Fig. 2, the vendor encrypts the design file using a design file encryption system, where a file header assembler accepts information to be placed in a file header into the encrypted design file. The information to be placed in the file header includes key information that gives information related to the decryption key, which information is to be used by the system in decrypting the encrypted design file. The creation of the encrypted design file comprising, encrypting the design file (control program code) into the encrypted design file using the design encryption key and appending the Tag A and

Tag B to the front of the encrypted design file [col. 6 lines 6-28]. The vendor safely supplies the encrypted version of the design file to his/her customers. The design processing engine obtains the design information and performs processing upon the design information from the encrypted design file [Fig. 4]. The design processing engine performs the following steps: reconstructs the design decryption key, verifies correctness of the design decryption key by recreating Tag B and confirms that the recreated Tag B is identical to the Tag B found in the header of the encrypted design file, decrypting the encrypted design file using the design decryption key [col. 7 line 55-col. 8 line 19]. Therefore, Redman teaches editing of the encrypted program as above. Further, Parlour's invention relates to secure configuration data used to configure a programmable logic device. When a user completes the design of the user specific circuit that incorporates the IP module (control program code). A configuration data bitstream is to be generated so that it can be send to the target PLD to configure the target PLD. The license manager encrypts the IP module portion (i.e. partially encrypted) of the bitstream using the ID module key [col. 4 lines 34-44]. The license manager also inserts into the bitsream the key number of the IP module key in such a way that the key number is associated in the bitstream with the encrypted IP module portion [Fig. 6]. The target PLD receives the bitstream including the key number and the encrypted IP module portion. The target PLD uses the key number to retrieve the proper ID module key, and then uses the retrieved IP module key to decrypt the IP module portion [col. 4 lines 45-52]. Therefore, Parlour teaches partially encryption (or encrypting a part of control program) and decryption process on the control program code as

above. In this case, the combination of Redman and Parlour teaches the claim limitation and the combination is sufficient to incorporate the teaching of Parlour into the teaching of Redman to encrypt a part of a control program code and decrypt the partially encrypted control program. The modification would be obvious because one of ordinary skill in the art would be motivated to prevent replicating the user's specific design by unscrupulous second user's copied bitstream to configure another product [Parlour, col. 2 lines 17-26].

For the above reasons, it is believed that the rejections should be sustained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Respectfully submitted,

Patel Nirav N. Patel

8/22/07

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

Gilberto Barron
SPE 2132

/Benjamin Lanier/
Benjamin Lanier
Patent Examiner, GAU 2132